Keynote Address by Commissioner Julie Brill
United States Federal Trade Commission

IAPP's Second Annual Conference:
"The FTC and Consumer Privacy Protection"
Washington, DC

December 7, 2010

Good morning. Thank you for that kind introduction and for the opportunity to speak on privacy. I have spent considerable time working on and thinking about privacy, and I am thrilled to have landed at the FTC, the agency leading the federal government's efforts on it.

In light of the season, I would like to reflect on the FTC's privacy agenda through the lens of our new American holidays, Black Friday and Cyber Monday. I don't know about you, but I survived them relatively unscathed. I picked up a couple of deals for the boys at Best Buy, but that was about it.

I had nothing like the Black Friday that Gail Grenon had. She got in line at Walmart at 2:45 AM, didn't get into the store until 5 AM, but was still able to buy a 32-inch, flat screen TV for $198. Jennifer Hernandez got a pair of Frye boots she was going to buy from Zappos.com but found them at Stella's, near her Saratoga Springs home, for 50% off. Harry Brelsford of Bainbridge Island, Washington, on the other hand, waited until Cyber Monday to buy a Briggs-Stratton 87-50 portable generator; he was definitely influenced by the recommendation in *Consumer Reports*, but the free shipping from Amazon.com sealed the deal for him.

These individuals are not friends of mine. I only know about them from what they chose to tell the world on blogs or websites. Just a couple of quick Google searches turned up literally thousands of detailed descriptions of thousands of consumers' thoughts and purchases on Black Friday and Cyber Monday. And I didn't even check Twitter.

This sort of online exhibitionism doesn't happen only on the high holy days of consumerism. The Internet is full of painfully detailed information proffered by consumers on what they are buying, where, why, and for how much. There are even short films — and some not so short — of teenage girls holding up everything they bought at the mall that day. And I was stunned to find a series of blogs in which young career women itemize their monthly expenditures, accompanied by graphs showing their exact net worth and tickers counting down their student loans.

When I was growing up, it was considered rude to talk about your salary or what you paid for something. Although those days are clearly gone, there are — despite the impression one gets when searching the Internet — many consumers who wish to keep information about their purchases and shopping habits to themselves.

Still, it is fair to ask: Why — when cyberspace is a cacophony of some consumers sharing every detail of their buying behavior — does the FTC call for new industry practices, stricter rules, and maybe even new laws to protect the privacy of consumer information?

The answer is simple: Because we at the FTC believe that individuals' privacy — which includes their identity, their shopping decisions, their browsing habits, how they choose to present themselves to the world — is of great value. Our belief in the value of privacy is deeply rooted. Supreme Court Justice Louis Brandeis wrote that our founding fathers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations" — and did so by conferring on us "the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."[1]

Of course, if Justice Brandeis were with us today, he would see the activities of Gail Grenon, Jennifer Hernandez, Harry Brelsford, and countless other Americans as consistent with the principles of privacy. Gail, Jennifer and Harry recount their shopping adventures online because they choose to make public what they have a right to keep private.

This brings me to another bedrock principle in American society that we seek to promote at the FTC. In America, we do not allow people to take things of value from others without their permission. At the FTC, one of our primary missions is to translate that principle into the marketplace; we make sure consumers have the information they need in order to never give up more than they intended or get back less than they were promised. This principle, the right to make informed choices about when to give up something of value — be it money or privacy — is the touchstone of our report, entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."[2]

Background

Since the enactment of the Fair Credit Reporting Act in 1970,[3] the FTC has led the federal government's efforts to protect consumer privacy. Section 5 of the FTC Act empowers us to challenge deceptive or unfair acts or practices.[4] We also enforce a number of sector-specific laws, including those that protect personal information about children[5] and consumer data used in credit, employment, and other sensitive financial transactions.[6] We implement the CAN-SPAM Act,[7] which seeks to limit unwanted and deceptive email, and we run the national Do Not Call Registry,[8] which Dave Barry has called the most popular government program since the Elvis stamp.

---

[1] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[2] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) (preliminary FTC staff report), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[3] 15 U.S.C. § 1681.

[4] 15 U.S.C. §§ 41-58.

[5] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6508 (1998).

[6] 15 U.S.C. § 1681.

[7] 15 U.S.C. § 7701.

[8] The Telemarketing Sales Rule, 16 C.F.R. Part 310 (2002).

Throughout the years, the Commission has worked to preserve consumers' control over their private data, even as technology races ahead, and the marketplace constantly develops new ways to collect, aggregate and use that data. In the 1990s, we relied primarily on a "notice and choice" model, counting on businesses to give consumers clear choices about how their data is used, and counting on consumers to read and understand privacy policies before making those choices.

The theory seems sound on its face, but it has proven unworkable. It is unreasonable to expect consumers to read and understand privacy policies — most about as long and as clear as the Code of Hammurabi — especially when all that stands between them and buying that new flat-screen TV or cute pair of boots is checking the little box that says "I consent."

So, a bit after the beginning of this century, the Commission turned to playing defense — focusing on privacy violations that cause indisputable harm: data breaches, identity theft, invasions of children's privacy, spam, spyware, and the like. But this approach falls short as well. It only addresses infringements on privacy *after* harm has been done, giving too little incentive to companies to design systems that don't do harm in the first place. Also, by focusing only on tangible harms to consumers, this approach misses the less quantifiable — but nonetheless real — injuries suffered by the exposure of sensitive information such as data relating to medical conditions, children, or sexual orientation.

And both approaches have fallen short as our technology advances, presenting ever more sophisticated opportunities to manipulate data, including the ability to take information that has been stripped of personal identification and re-associate it with specific individuals.

The Report

With the FTC's "notice and choice" and "no harm, no foul" paradigms falling short of providing meaningful privacy protection for consumers in this advanced technological age — allowing more and more rapid data collection that is more and more invisible to consumers — the Commission proposed an updated framework for safeguarding consumers' personal data.

The report makes three principal recommendations. We call for companies to build privacy protections into their everyday business practices. We call for simplified privacy policies that consumers can understand without having to retain counsel. And we call for greater transparency around data collection, use, and retention.

When taken as a whole, I believe the framework we have proposed is flexible enough to allow both businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace. This is an important point. The Commission recognizes that many of the practices at issue — including behavioral advertising — provide real benefits to consumers. And we do not want to stifle innovation. But some of the practices raise serious concerns. So we have sought to balance the competing interests.

Do Not Track

The Commission's most talked-about recommendation is the creation of a "Do Not Track" mechanism that would allow consumers some meaningful control over how their online information is used. I am guessing this is the proposal of interest to most of you in this room, and I want to dispel some concerns we have already heard about it.

The first is the technological feasibility of "Do Not Track." I would agree that this could be a problem if "Do Not Track" were precisely modeled on our "Do Not Call" registry, which relies on a list of unique identifiers in the form of telephone numbers. But there are no comparable identifiers for computers, and creating them would raise its own significant set of privacy issues.

Instead, the Commission recommends using a browser-based approach, which has a couple of advantages. It will allow consumers to make persistent choices using something like a cookie that travels with them through cyberspace, communicating their tracking preferences to every website they visit. And such an approach would allow consumers more granular choices, beyond just opting out of behavioral advertising altogether. Consumers could have meaningful control over the information they share and the sort of targeted ads they receive. I want to commend the browser providers who have been experimenting with how to provide these controls to consumers in a more user friendly, meaningful way. I expect that, in the very near future, we will see more dramatic progress in this area from the browser providers. So let's not spend too much time debating whether our recommended approach is technologically feasible.

This brings me to a second concern we have heard about "Do Not Track" — that, given the choice, consumers en masse will opt out of behavioral advertising, drying up the ad revenue that lets us enjoy content and innovative online activities for free.

As the Commission learned during the privacy roundtables, when given an informed and more granular choice, most consumers, including myself, want to receive tailored ads — and will choose to share information for that purpose.

This entire discussion about the dilemma advertisers believe they are in reminds me of one of the quintessential movies of this season, "Miracle on 34th Street." For those of you too young to have seen it, the movie is about a Macy's Santa Claus who listens to children's Christmas wishes, then sends their parents to other stores if Macy's doesn't have exactly what their children want. Of course, the personal attention is a huge hit with shoppers. Mr. Macy himself says: "No high pressuring and forcing a customer to take something he doesn't really want. We'll be known as the helpful store . . . the store that places public service ahead of profits. And, consequently, we'll make more profits than ever before."

Mr. Macy would not have had a problem with "Do Not Track." He would have recognized that providing consumers with meaningful choices increases his credibility and can grow, rather than shrink, his market share. He would have been eager to compete with respect to privacy.

"Do Not Track" provides an opportunity to a business or ad network to convince consumers that it will handle their personal data with care and put the information to good use in serving them, so that consumers will not want to opt out. I have no doubt the marketing departments of companies selling on the Internet, and their ad networks, are up to the task of creatively informing consumers about the benefits of collecting and using their information to provide more personalized advertising. The alternatives — not informing consumers about what is happening, or obscuring the truth and creating obstacles to making choices — are simply not palatable.

Legislation for and Regulation of Do Not Track

So, is Congressional action needed to mandate a Do Not Track mechanism, or can we simply wait for industry to come up with one on its own? To be sure, Internet companies *could* create a robust, broad-based self-regulatory system and require that members pledge to honor consumer choices through their browser cookies. And as you all know, the FTC has the authority under current law to enforce promises made to consumers in a self-regulatory framework.

However, despite what I believe are obvious marketing advantages to providing consumers with clear, simple, just-in-time notices and choices about behavioral advertising, the industry has been slow to adopt a uniform and comprehensive framework. I want to commend those companies who have risen to the challenge thus far. However, the recent chest-pounding and hair-pulling we have heard and seen from some industry players over the "Do Not Track" recommendation suggests that the attitude of some members of industry — including some significant players — is not going to change easily or quickly. And even if a good number of the companies operating in cyberspace did voluntarily commit to a "Do Not Track" system, there would likely be a few that would not join, and hence not fall under the FTC's "promises made, promises broken, time to enforce" jurisdiction.

So back to my question: Does Congress need to act? Here is my position: If the browser vendors and advertisers don't endorse a robust and uniform Do Not Track mechanism, I will support legislation to mandate it. In my view, Congress has a number viable options: Congress itself can create the contours of "Do Not Track." Or it can simply require the Commission to craft a rule. The "Do Not Track" mechanism can even allow for a safe harbor for a robust, industry-created notice and choice system approved by the Commission. Whichever of these options it chooses, Congress should give the Commission APA rulemaking authority and the ability to seek civil penalties to enforce "Do Not Track." The goal is to end up with a browser-based system that gives consumers understandable, simple, and easy-to-find choices about how their personal data will be used when they are online — and that gives the FTC the teeth we need to ensure all advertisers and websites honor those choices.

As I mentioned, the report discusses many important privacy issues, concerning both online and offline information. If Congress decides to undertake a full examination of these privacy concerns, the entire FTC report would serve as a very good basis for such a Congressional review.

Data Collection and Information Brokers

But there is one other aspect of the report I want to highlight in particular. To provide greater transparency, we recommend that consumers be allowed reasonable access to the information collected about them by companies. As you know, the report calls for that access to be proportional to both the sensitivity of the data and how it is to be used. This is particularly important with respect to information brokers — entities that never engage consumers directly and are often invisible to them. Yet these companies control details about consumers that can have a direct impact on their credit and financial well being.

I believe we may need to modernize our notions about information brokers, and perhaps even credit reporting agencies, to keep up with new methods of collecting, selling, and using information about consumers for decisions about financial products. We hear and read about businesses that "scrape" and "sniff" for information about particular consumers on the Web, including on social network sites, and provide that information to insurers, lenders, and other financial firms. These financial firms then use this information in making decisions about whether — and on what terms — to provide financial products to these consumers.

When Congress created the Fair Credit Reporting Act, it created clear guidelines on how personal information can be used for credit, insurance and other financial services. Congress mandated that consumers have a right to know when it is being used, and a right to access and correct it. The Federal Trade Commission and the new Consumer Financial Protection Bureau need to make sure our current rules continue, in this technologically advanced age, to protect consumers' rights under the FCRA — both the right to know the data that has been collected and used in making important financial decisions, and to correct that data when necessary.

Conclusion

Each year, we Americans move more of our lives online. We are friends with people whose voices we've never heard. We tweet our thoughts to a cyber café full of strangers. Where teens once hid diaries under their beds, they now post them online for everyone to read, except their mothers who can't figure out how to break through the privacy settings. Shops email us when it is our grandmother's birthday, remind us what we got her last year, suggest a present for this year, and offer to charge it on our credit card they stored.

We shop for groceries online, go to the movies online, share photo albums online, date online, and pay traffic tickets online.

No doubt, this trend will continue. But just because more and more Americans are choosing to share more of their personal information online does not mean we all agree — or should agree — to give up control over that data.

At the FTC we are committed to protecting consumers' privacy by safeguarding their right to choose what they reveal about themselves in the marketplace, and how that information is used. I believe the Commission's proposed new framework, including the "Do Not Track"

proposal, furthers that goal. And while I still hope industry will rise to the challenge of protecting their customers' privacy, this issue has become too important — to the FTC's central mission and to consumers across the country — for us to continue to wait. If industry does not move in a meaningful way on this issue, I will not hesitate to call on Congress to provide consumers with meaningful notice and choice about how their information is used, and to give the FTC the enforcement tools it needs to make sure those choices are respected.

Thank you.